

Asymptotically optimal purification and dilution of mixed qubit and Gaussian states

Peter Bowles,* Mădălin Guță, and Gerardo Adesso
*School of Mathematical Sciences, University of Nottingham,
 University Park, Nottingham NG7 2RD, United Kingdom*

(Dated: March 21, 2011)

Given an ensemble of mixed qubit states, it is possible to increase the purity of the constituent states using a procedure known as state purification. The reverse operation, which we refer to as dilution, produces a larger ensemble, while reducing the purity level of the systems. In this paper we find asymptotically optimal procedures for purification and dilution of an ensemble of independently and identically distributed mixed qubit states, for some given input and output purities and an asymptotic output rate. Our solution involves using the statistical tool of local asymptotic normality, which recasts the qubit problem in terms of attenuation and amplification of a single-mode displaced Gaussian state. Therefore, to obtain the qubit solutions, we must first solve the analogous problems in the Gaussian setup. We provide full solutions to all of the above, for the (global) trace-norm figure of merit.

PACS numbers: 03.67.Hk, 03.65.Wj, 02.50.Tt, 42.50.Dv

I. INTRODUCTION

When implementing any quantum information protocol, the states we wish to employ and manipulate are inevitably affected by decoherence effects, which diminish their purity and consequently their resource power. There exist several well-established methods to protect against such undesirable factors: strengthening the entanglement resource using distillation methods [1] or employing a quantum error correction scheme [2] to encode our ‘fragile’ states into some larger, more unyielding system. The method we study in this paper is that of state *purification* [3, 4], a procedure which takes as input an ensemble of identical copies of an arbitrary (unknown) state and produces as output a smaller ensemble of identical states with higher purity. This can be seen as a special case of the more general problem of inverting the effect of a noisy channel on ensembles of states, the channel being the depolarising one in the present study.

There already exists several theoretical results for purification of n i.i.d. (independently and identically distributed) mixed qubits, notably Refs. [3, 4], where optimal purification algorithms for various formulations of the purification problem are provided. Purification of an ensemble of mixed qubit states has also been found to occur in the context of ‘superbroadcasting’ [5], an $n \rightarrow m$ cloning procedure which can actually result in purified clones for $n \geq 4$ and sufficiently mixed input states (the noise present is merely shifted from local states into correlations between output states). For $n \geq m$, superbroadcasting is actually equivalent to the optimal purification procedure of [3]. Experimentally, purification has been achieved in [6], which implemented the methodology of [3] and demonstrated optimal purification for the case $n = 2$.

Beyond the *entanglementology* (phenomenology of entanglement), judging the performance of a purification protocol requires a figure of merit (FoM) which measures the departure

from the ideal transformation. Two types of FoM have been considered in the literature, with very different results. The *local* FoM is built upon the comparison of the *reduced* states of individual output systems with the target state. In this case, a complete reversal of the depolarising channel may be obtained asymptotically with the size of the input ensemble, and with arbitrarily high output rate m/n [4]. The *global* FoM compares the *joint* state of the output with that of a product of independent target states. This is a more demanding criterion. For example if the output systems are independent and identically prepared then the global fidelity scales as $F(n, m) = F_n^m$ where $F_n < 1$ is the fidelity of an individual output state with respect to the target state. Indeed, it has been shown [4] that no protocol can achieve asymptotic purification ($F(n, m) \rightarrow 1$) to *pure* target states at a finite rate m/n . The global figure of merit is relevant whenever we deal with the collective state of the output rather than the individual constituents, as in the case of state transfer between atomic ensembles and light. Additionally, it can serve as a “measure of correlations” when the individual constituents of the output states are known to be exactly in the target state, as in superbroadcasting. This hypothesis will however not be pursued in this paper.

The above no-go theorem motivates us to consider the question whether the depolarising channel can be reversed with a positive asymptotic output rate, when the target states (i.e. the states prior to applying the depolarising channel) are *mixed*. We show that this is indeed possible, and compute the maximal purification rate for given input and target purity, and the optimal FoM for approximate purification at a fixed rate which is higher than the maximal one.

We also consider the opposite process of *dilution* in which, starting from an ensemble of n identically prepared states, we produce a *larger* ensemble consisting of m independent, but more mixed states. Dilution shares similarities with the process of optimal $n \rightarrow m$ quantum cloning [7], but while in cloning the rate m/n is fixed, and one aims at generating clones as close as possible to the input states (with respect to a local or a global FoM), in a dilution procedure we set a target level of output purity and look for the optimal rate for generating such target states.

*Corresponding author.

Electronic address: pmxpb2@nottingham.ac.uk

	qubit problem	Gaussian problem
state model	ensemble of n i.i.d mixed qubits $\rho_{\mathbf{r}}^{\otimes n}$ [Eq. (16)] $n \gg 1$: number of copies \mathbf{r} with $\ \mathbf{r}\ \leq 1$: Bloch vector;	single-mode displaced Gaussian state Φ_{α}^s [Eq. (7)] $\alpha \in \mathbb{C}$: displacement; $s \in (0, 1)$: purity parameter
input	$\rho_{\mathbf{r}_0 + \mathbf{u}/\sqrt{n}}^{\otimes n}$	$\Phi_{\alpha}^{s_1}$
target	$\rho_{\lambda \mathbf{r}_0 + k\mathbf{u}/\sqrt{m}}^{\otimes m}$	$\Phi_{k\alpha}^{s_2}$
procedure	purification $\lambda > 1, m < n$	attenuation $s_2 < s_1, k < 1$
procedure	dilution $\lambda < 1, m > n$	amplification $s_2 > s_1, k > 1$

TABLE I: Summary of the notation adopted in the present paper. For the qubit problem, we aim at optimising the output-vs-input rate m/n (maximising it for purification, and minimising it for dilution) at given input Bloch vector $\mathbf{r}_0 + \mathbf{u}/\sqrt{n}$ and scale factor λ . For the corresponding Gaussian problem, we aim at finding the maximal value of the displacement ratio k , such that attenuation or amplification can be realised perfectly, for given target temperature parameters s_1 and s_2 and unknown displacement α . The framework of local asymptotic normality provides a rigorous link between the two problems, as for $n \gg 1$ the local Bloch vector \mathbf{u} is mapped into the displacement α of a single-mode coherent thermal state.

In deriving the asymptotic results, the key mathematical tool is that of local asymptotic normality (LAN), a fundamental ‘classical’ statistics technique [8] which was recently extended to the context of quantum statistical models [9–12]. In the quantum case, LAN dictates that the collective state of n i.i.d. quantum systems, can be approximated by a joint Gaussian state of a classical and a quantum continuous variable (CV) systems. This has been used to derive asymptotically optimal state estimation strategies for mixed states of arbitrary finite dimension [11], and also in finding quantum teleportation benchmarks [14] and optimal quantum learning procedures [15] for multiple qubit states. The general strategy is to recast statistical problems involving n i.i.d. quantum systems into the simpler setting of Gaussian states. The optimal solution for the corresponding Gaussian problems can then be used to construct asymptotically optimal procedures for the original one. In section III we sketch how this could be physically implemented, and more details can be found in [10].

Following this methodology, we transform the qubit purification and dilation problems into those of optimal *attenuation* and *amplification* for a one-mode CV system in a Gaussian state, together with a classical real-valued Gaussian variable, both with known variance but unknown means. In attenuation we reduce the variance of a displaced Gaussian state, at the price of simultaneously reducing its amplitude, while in amplification we increase the amplitude, as well as the variance. For both problems we use a FoM based on maximum trace-norm distance, and show that the optimal attenuation channel is obtained by applying a beamsplitter, while the optimal amplification is implemented by a non-degenerate parametric amplifier. A similar scheme for the attenuation of Gaussian CV states has been proposed and experimentally implemented in [16]. Parametric amplification has been investigated in [17–19], and demonstrated experimentally in [20]. In particular, the same amplifier is optimal for a FoM based on the mini-

mum amount of added noise [17, 18]. However, whilst these transformations are well known candidates for our protocols, to the best of our knowledge a proof of their optimality with respect to the FoM chosen in this paper had not been obtained in the literature. Our proof relies on a covariant channels optimisation technique developed in [14, 21]. We find that for given input and output purity parameters, there exists a range of values for the ratio k between output and input displacement, such that attenuation or amplification can be realised perfectly, and we compute the maximal (optimal) value k_0 , as a function the two purities. In the parameter range where the procedures cannot be accomplished perfectly, we give the exact expression for the optimal FoM.

A schematic summary of the problems addressed in this paper is provided in Table I. The paper is organised as follows. In Section II we formulate and solve the two quantum Gaussian problems, and the corresponding classical one. In Section III we use this result in conjunction with LAN to find asymptotically optimal purification and amplification channels for states of n i.i.d. mixed qubits. We draw our concluding remarks in Section IV. The proofs are collected in Appendix A.

II. OPTIMAL ATTENUATION AND AMPLIFICATION OF GAUSSIAN STATES

A. Classical Case

Before we move onto the quantum case, it is instructive and relevant to consider the corresponding problems for classical random variables. In the classical scenario, the analogue of ‘attenuation’ (‘amplification’) is a procedure which reduces (increases) the mean and variance of a given random variable. The analogue to our quantum problem would then be to find a transformation K which maps a real-valued normally dis-

tributed random variable $X \sim N(u, V_1)$ of arbitrary mean u and fixed variance V_1 , into a variable $Y \sim N(ku, V_2)$ such that the risk

$$R_{\max}(K; V_1, V_2, k) = 2 \sup_u \|K(N(u, V_1)) - N(ku, V_2)\|_{\text{tv}} \quad (1)$$

is minimised. Here k represents a fixed constant, where $0 < k < 1$ means attenuation and $k > 1$ means amplification of the Gaussian variable X , and we choose the interesting case where $V_1 > V_2$ in the case of attenuation, and $V_1 < V_2$ for amplification. The notation $\|\mathbb{P} - \mathbb{Q}\|_{\text{tv}} = \sup\{|\mathbb{P}(A) - \mathbb{Q}(A)| : A \in \mathcal{F}\}$, for the σ -algebra \mathcal{F} , represents the total variation distance between the probability distributions \mathbb{P} and \mathbb{Q} which reduces to one-half of the L_1 -distance between their probability densities in the case of mutually absolutely continuous distributions [22].

The solutions of both classical and quantum versions of this problem rely on the notion of ‘covariance’. Consider the transformation

$$X \mapsto K(X) = kX + Z \quad (2)$$

where X and Z are independent random variables, Z having a fixed variance and vanishing mean. Such a (classical) channel is covariant, in the sense that

$$K(X + C) = K(X) + kC \quad (3)$$

for any constant C . Such transformations can be shown to not only minimise (1), but also to render it independent of expectation so that the FoM becomes

$$R_{\max}(K; V_1, V_2, k) = 2\|K(N(0, V_1)) - N(0, V_2)\|_{\text{tv}}.$$

It is easy to see that if

$$k \leq k_0^{(c)}(V_1, V_2) := \sqrt{\frac{V_2}{V_1}} \quad (4)$$

then the target distribution can be achieved exactly, with the appropriate amount of Gaussian noise in the variable Z . As we shall see in the next section, there exists an analogous range (12) for the quantum Gaussian transformation.

As for the case $k > k_0^{(c)}(V_1, V_2)$, it can be shown [22] that the optimal choice for Z in (2) is $Z = 0$, as one would expect, so that the optimal figure of merit is

$$R_{\min\max}(V_1, V_2, k) := \inf_K R_{\max}(K; V_1, V_2, k) = \int \left| \frac{1}{\sqrt{2\pi k^2 V_1}} e^{-\frac{x^2}{2k^2 V_1}} - \frac{1}{\sqrt{2\pi V_2}} e^{-\frac{x^2}{2V_2}} \right| dx. \quad (5)$$

Henceforth, we will denote by K^* the optimal transformation for the two cases discussed above.

B. Quantum Case

In this Section we consider the following: given a Gaussian state Φ_α of a one-mode CV quantum system, with known covariance and unknown displacement α , we would like to optimally attenuate (amplify) it, that is transform it into a state

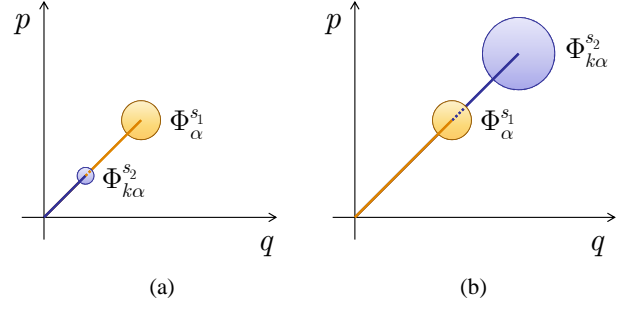


FIG. 1: (Color online) Schematic phase-space diagram for (a) attenuation and (b) amplification of a displaced Gaussian state $\Phi_\alpha^{s_1}$.

with smaller (greater) covariance and displacement $k\alpha$, with the largest possible proportionality constant k . Let

$$W_\alpha := \exp(\alpha a^\dagger - \bar{\alpha} a)$$

denote the Weyl operators where $\alpha \in \mathbb{C}$ and a, a^\dagger the creation and annihilation operators satisfying $[a, a^\dagger] = 1$ and

$$a|n\rangle = \sqrt{n}|n-1\rangle, \quad n \geq 0,$$

where $\{|n\rangle\}_{n \geq 0}$ is the Fock basis of the Hilbert space \mathcal{H} . For $0 < s < 1$ we denote by Φ^s the centred, phase invariant Gaussian state

$$\Phi^s = (1-s) \sum_{n=0}^{\infty} s^n |n\rangle\langle n|, \quad (6)$$

and by displacing it we obtain the family of Gaussian states

$$\Phi_\alpha^s := W_\alpha \Phi^s W_\alpha^\dagger. \quad (7)$$

Given two different mixing parameters $s_1 > s_2$ ($s_1 < s_2$) and a positive parameter $k < 1$ ($k > 1$) we would like to find the optimal attenuation (amplification) channel which maps the state $\Phi_\alpha^{s_1}$ close to the state $\Phi_{k\alpha}^{s_2}$ for an arbitrary displacement α (see Fig. 1). For any channel $P : \mathcal{T}_1(\mathcal{H}) \rightarrow \mathcal{T}_1(\mathcal{H})$ we define the FoM called the maximum risk

$$R_{\max}(P; s_1, s_2, k) = \sup_{\alpha \in \mathbb{C}} \|P(\Phi_\alpha^{s_1}) - \Phi_{k\alpha}^{s_2}\|_1 \quad (8)$$

and the minimax risk

$$R_{\min\max}(s_1, s_2, k) = \inf_P R_{\max}(P; s_1, s_2, k). \quad (9)$$

A channel is called ‘minimax’ if its maximum risk is equal to the minimax risk. We will show that (up to a trivial adjustment for a certain range of k ’s) the optimal solutions to the attenuation and amplification problems are, respectively, the beamsplitter and parametric amplifier.

We start by defining a specific channel denoted in both cases P^* , then show that it is optimal and compute the minimax risk. For $s_1 > s_2$ and $k < 1$, the attenuation channel is implemented by the action of a beamsplitter with reflectivity k acting on an input mode a prepared in a state $\Phi_\alpha^{s_1}$, and a

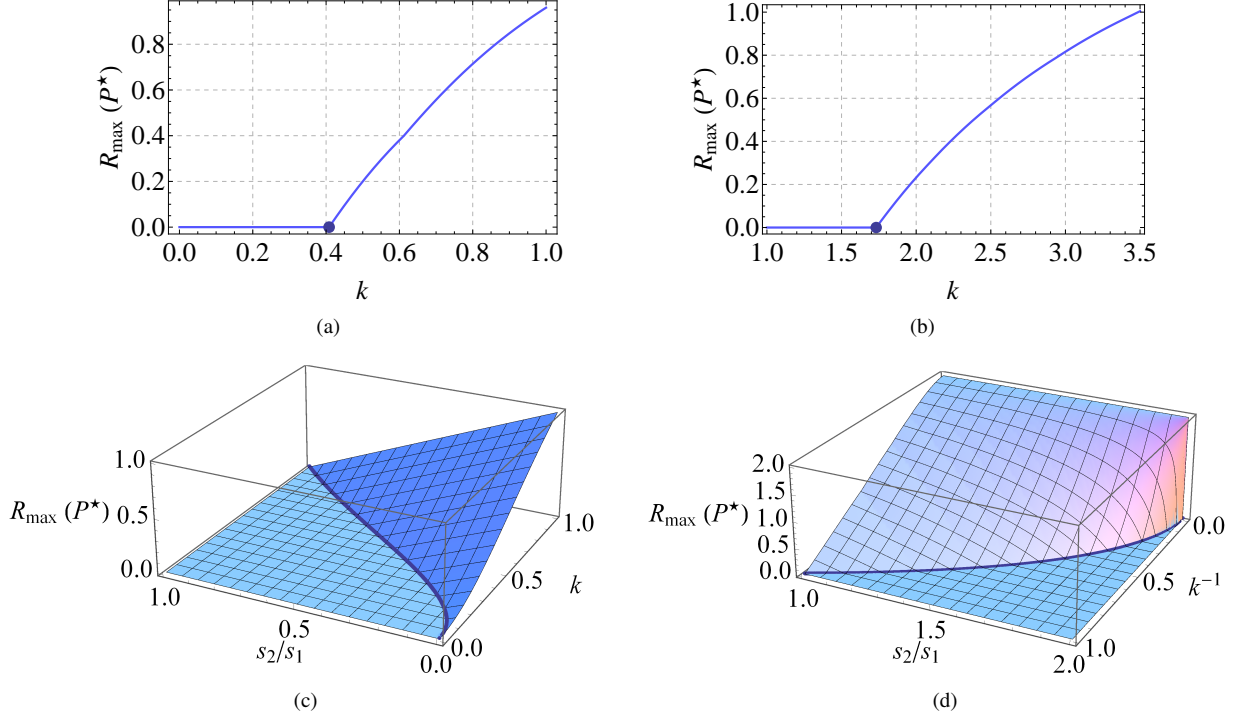


FIG. 2: (Color online) FoM's for optimal attenuation (left) and optimal amplification (right) of displaced Gaussian states. Top row: (a) Plot of the minimax risk R_{\max} [Eq. (14)] versus k for the optimal attenuation procedure P^* , where $s_1 = 0.8$ and $s_2 = 0.4$; the optimal value k_0 is highlighted with a big dot on the graph. (b) Plot of the minimax risk R_{\max} [Eq. (14)] versus k for the optimal amplification procedure P^* , where $s_1 = 0.4$ and $s_2 = 0.8$; the optimal value k_0 is highlighted with a big dot on the graph. Bottom row: 3D Plots of the minimax risk R_{\max} versus the parameter k and the output/input temperature ratio s_2/s_1 with $s_1 = 0.5$, for (c) the optimal attenuation procedure, and (d) the optimal amplification procedure; in both plots, the thick curve depicts k_0 as a function of s_2/s_1 .

second ancillary mode b in the vacuum state $\omega = |0\rangle\langle 0|$. The output mode c of the channel is

$$c = k^2 a + \sqrt{1 - k^2} b. \quad (10)$$

For $s_2 > s_1$ and $k > 1$, the channel is a parametric amplifier, whose action is represented by the following transformation on the input mode a and an ancillary mode b prepared in the vacuum state:

$$c = ka + \sqrt{k^2 - 1} b^\dagger. \quad (11)$$

We note that for each pair (s_1, s_2) there exists a range of parameters k for which $R_{\min\max}(s_1, s_2, k) = 0$, i.e., the procedures can be accomplished perfectly. Indeed it can be easily verified that, for k given by

$$k_0^{\text{att}}(s_1, s_2) = \sqrt{\frac{s_2(1-s_1)}{s_1(1-s_2)}}, \quad k_0^{\text{amp}}(s_1, s_2) = \sqrt{\frac{1-s_1}{1-s_2}}, \quad (12)$$

the channels (10) and respectively (11) produce exactly the target state $\Phi_{k\alpha}^{s_2}$. Moreover, if $k < k_0$ then the output of P^* is the state $\Phi_{k\alpha}^s$ with $s < s_2$, and the target can be still perfectly achieved by adding an appropriate amount of Gaussian noise. For later use, when $k < k_0$ we will denote by the same symbol P^* this modified channel. From now on we consider

the less trivial situation $k \geq k_0$, corresponding to the regime where perfect amplification or attenuation are impossible. We then state the following theorem and lemma, whose proofs are given in Appendix A:

Theorem II.1. *If $k < k_0$ then the minimax risk for attenuation (amplification) is zero. If $k \geq k_0$, the minimax procedure is P^* , i.e. the beamsplitter (10) in the case of attenuation, or the parametric amplifier (11) in the case of amplification:*

$$R_{\max}(P^*; s_1, s_2, k) = R_{\min\max}(s_1, s_2, k). \quad (13)$$

Lemma II.2. *If $k < k_0$, then the minimax risk for attenuation (amplification) is given by*

$$R_{\min\max}(s_1, s_2, k) = 2(\tilde{s}^{m_0+1} - s_2^{m_0+1}), \quad (14)$$

where m_0 is the integer part of

$$\ln[(1 - \tilde{s})/(1 - s_2)] / \ln(s_2/\tilde{s}),$$

and \tilde{s} takes the values

$$\tilde{s}_{\text{att}} = \frac{s_1 k^2}{1 - s_1 + s_1 k^2}, \quad \text{and} \quad \tilde{s}_{\text{amp}} = 1 - \frac{1 - s_1}{k^2}. \quad (15)$$

in the case of attenuation and respectively amplification.

The risk for both processes is plotted in Fig. 2 [(a)-(d)]. In Figure 3 we plot k_0 for both processes as a function of the input and output purity parameters s_1 and s_2 .

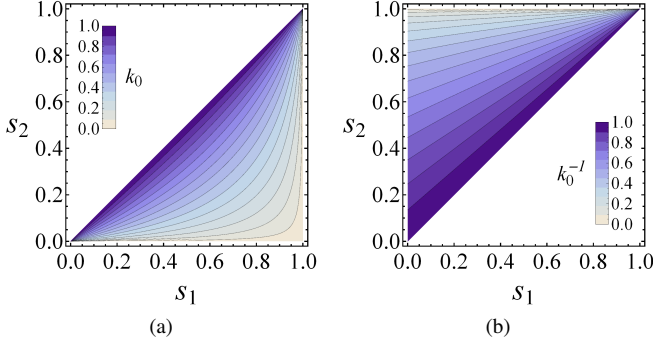


FIG. 3: (Color online) Contour plots of (a) k_0 versus the purity parameters s_1 and s_2 for the optimal attenuation procedure, and (b) k_0^{-1} versus the purity parameters s_1 and s_2 for the optimal amplification procedure.

III. ASYMPTOTICALLY OPTIMAL PURIFICATION AND DILUTION FOR ENSEMBLES OF QUBITS

We turn now to the problem of finding optimal purification and dilution schemes for ensembles of identical qubits. We denote by $\rho_{\mathbf{r}}$ the qubit state with Bloch vector $\mathbf{r} = (r_x, r_y, r_z)$

$$\rho_{\mathbf{r}} = \frac{1}{2}(\mathbf{1} + \mathbf{r}\boldsymbol{\sigma}), \quad (16)$$

where $\mathbf{r}\boldsymbol{\sigma} = r_x\sigma_x + r_y\sigma_y + r_z\sigma_z$ and σ_i are the Pauli matrices. We are given n identical qubits prepared in the state $\rho_{\mathbf{r}}$ and we would like to produce m identical qubits in the state $\rho_{\lambda\mathbf{r}}$ with m as large as possible, for a fixed positive parameter λ . When $\lambda > 1$, the aim is to “purify” the state, and when $0 < \lambda < 1$ we want to “dilute” the state with the benefit of obtaining more copies. Clearly, for purification the output state is physical only if λ satisfies $\lambda\|\mathbf{r}\| \leq 1$. This can be achieved by letting λ depend on \mathbf{r} , or by restricting to those input states which satisfy the property. To illustrate the latter, suppose we would like to reverse the action of the depolarising channel

$$C : \rho_{\mathbf{r}} \mapsto \rho_{\mathbf{r}/\lambda},$$

then the input states of the purification channel automatically satisfy the requirement. As to the former, our asymptotic analysis will produce a *local* FoM which only depends on the value of λ at a particular state, so for simplicity we will assume it to be constant.

A purification (dilution) procedure is a quantum channel

$$Q_n : M(\mathbb{C}^{2^n}) \rightarrow M(\mathbb{C}^{2^m})$$

mapping n -qubit states to m -qubit states, and its performance is measured by the FoM (risk)

$$R(Q_n; \mathbf{r}, \lambda) := \|Q_n(\rho_{\mathbf{r}}^{\otimes n}) - \rho_{\lambda\mathbf{r}}^{\otimes m}\|_1. \quad (17)$$

Note that this is a global rather than a local risk, in the sense that it measures the distance between the output and the *joint* product state, instead of comparing their restrictions to each

single system. Note also that the risk at a fixed point \mathbf{r} can always be made equal to zero by simply preparing the target state for that point. To take into account the *overall* performance of a procedure, one can either integrate the risk with respect to a prior distribution over states (Bayesian statistics) or take the maximum over all states (frequentist statistics). We adopt the latter viewpoint, and in addition we will consider a more refined version of the maximum risk called *local maximum risk* around \mathbf{r}_0

$$R_{\max}(Q_n; \mathbf{r}_0, \lambda) := \sup_{\|\mathbf{r} - \mathbf{r}_0\| \leq n^{-\frac{1}{2} + \epsilon}} R(Q_n; \mathbf{r}, \lambda). \quad (18)$$

In asymptotic statistics the local maximum risk is more informative than the ‘global’ one since it captures the behaviour of the procedure around any point in the parameter space, rather than that of the worst case. The radius of the ball over which we maximise is slightly larger than the precision of $n^{-1/2}$ with which we can estimate the state parameters, so that the definition of the local risk does not amount to assuming any prior information about the parameter. Indeed one can use a small sample $n^{1-\epsilon} \ll n$ of the input systems to obtain a rough estimate of the Bloch vector \mathbf{r} such that the obtained estimator \mathbf{r}_0 will be in a ball of size $n^{-1/2+\epsilon}$ around \mathbf{r} , with probability converging to one as $n \rightarrow \infty$. With this additional information, one can then apply the purification (dilution) channel to the remaining systems, with no loss in the asymptotic optimal risk (see below). The local maximum risk is a standard FoM in asymptotic statistics and it has been used in quantum statistics in [9, 10, 15] to which we refer for more details, and for its relation to Bayesian methods.

Up to this point the number of input and output systems n and m were fixed, with n considered to be large. However, for a non-trivial asymptotic analysis, m should be an increasing function of n , more precisely we consider the optimal purification (dilution) procedure for a fixed rate

$$\Lambda = \lim_{n \rightarrow \infty} \frac{m(n)}{n} > 0.$$

Indeed from our fixed rate analysis it can easily be deduced that in the case of a sub-linear dependence $m(n) = o(n)$, one can produce m output copies of arbitrary purity with vanishing local maximum risk. On the other hand, by similar reasonings, one may expect that if $m(n)/n$ is unbounded, then the best strategy should be to estimate the state and reprepare m independent copies of the estimator (‘measure and prepare’ strategy [23]). We leave this statement as a conjecture, and from now on we will assume that the rate Λ is given and fixed. For any sequence $\mathbf{Q} := \{Q_n\}$ of procedures we define the *asymptotic local maximum risk* at \mathbf{r}_0 by

$$R(\mathbf{Q}; \mathbf{r}_0, \lambda, \Lambda) := \limsup_{n \rightarrow \infty} R_{\max}(Q_n; \mathbf{r}_0, \lambda), \quad (19)$$

and we would like to find an optimal (minimax) strategy whose asymptotic risk is equal to the *minimax risk*

$$R_{\min\max}(\mathbf{r}_0, \lambda, \Lambda) := \limsup_{n \rightarrow \infty} \inf_{Q_n} R_{\max}(Q_n; \mathbf{r}_0, \lambda). \quad (20)$$

In other words, we will answer the following question: for given purification (dilution) constant scale factor λ and input-output rate Λ , what is the minimax risk $R_{\min\max}(\mathbf{r}_0, \lambda, \Lambda)$ and which is the procedure that achieves it? In particular, we will find that the minimax risk is zero for a range of parameters $(\mathbf{r}_0, \lambda, \Lambda)$, and we will identify the maximum value Λ_0^{pur} (Λ_0^{dil}) for which the purification (dilution) can be performed with asymptotically vanishing risk. These rates are the qubit analogues of the constants k_0 defined in (12).

The main technical tool is the theory of *local asymptotic normality* (LAN) developed in [9–12] as an extension of a key concept from (classical) asymptotic statistics [8, 24]. LAN means that the joint quantum state of identically prepared (finite-dimensional) systems can be approximated in a strong sense by a quantum-classical Gaussian state of fixed variance, whose mean encodes the information about the parameters of the original state. In this way, a number of asymptotic problems can be reformulated in terms of Gaussian states, for which the explicit solution can be found, e.g. state estimation [25], teleportation benchmarks [14], quantum learning [15], system identification [26]. For the purposes of this paper we give a brief description of LAN for mixed qubit states. Let

$$\rho_{\mathbf{r}_0 + \mathbf{u}/\sqrt{n}} = \frac{1}{2}(\mathbf{1} + (\mathbf{r}_0 + \mathbf{u}/\sqrt{n})\boldsymbol{\sigma})$$

denote a qubit state in the neighbourhood of a fixed and known state $\rho_{\mathbf{r}_0}$, which is uniquely characterised by an *unknown* local parameter \mathbf{u} . The family of n -qubit states

$$\mathcal{P}_n := \left\{ \rho_{\mathbf{u}}^n := \rho_{\mathbf{r}_0 + \mathbf{u}/\sqrt{n}}^{\otimes n} : \|\mathbf{u}\| \leq n^\epsilon \right\} \quad (21)$$

will be called the local statistical model at \mathbf{r}_0 . Additionally, we define a classical-quantum Gaussian model

$$\mathcal{N} := \{N_{\mathbf{u}} \otimes \Phi_{\mathbf{u}} : \mathbf{u} \in \mathbb{R}^3\} \quad (22)$$

where $N_{\mathbf{u}} := N(u_z, 1 - \|\mathbf{r}_0\|^2)$ is a normal (Gaussian) distribution on \mathbb{R} with mean u_z and variance $1 - \|\mathbf{r}_0\|^2$, and

$$\Phi_{\mathbf{u}} = W_{\alpha} \Phi^s W_{\alpha}^{\dagger}, \quad \alpha = \frac{u_x + iu_y}{2\|\mathbf{r}_0\|}, \quad s = \frac{1 - \|\mathbf{r}_0\|}{1 + \|\mathbf{r}_0\|},$$

is a displaced thermal Gaussian state of a one-mode CV system (cf. Section II B) with known covariance matrix characterised by the purity parameter s (with zero squeezing) and unknown means proportional to (u_x, u_y) . Now, the mathematical statement of LAN [9] is that there exist two sequences of channels $\mathbf{T} = \{T_n\}$ and $\mathbf{S} = \{S_n\}$ with

$$\begin{aligned} T_n &: M(\mathbb{C}^{2^n}) \rightarrow L^1(\mathbb{R}) \otimes \mathcal{T}_1 \\ S_n &: L^1(\mathbb{R}) \otimes \mathcal{T}_1 \rightarrow M(\mathbb{C}^{2^n}) \end{aligned}$$

such that

$$\begin{aligned} \lim_{n \rightarrow \infty} \sup_{\|\mathbf{u}\| \leq n^\epsilon} \|T_n(\rho_{\mathbf{u}}^n) - N_{\mathbf{u}} \otimes \Phi_{\mathbf{u}}\|_1 &= 0, \\ \lim_{n \rightarrow \infty} \sup_{\|\mathbf{u}\| \leq n^\epsilon} \|\rho_{\mathbf{u}}^n - S_n(N_{\mathbf{u}} \otimes \Phi_{\mathbf{u}})\|_1 &= 0. \end{aligned}$$

In the above formulas, \mathcal{T}_1 is associated to the trace-class operators of the CV system, and the norm-one $\|\cdot\|_1$ denotes respectively the trace-norm for the quantum part and the L_1 -norm for the classical part. The physical implementation for the channels T_n and S_n , detailed in [13], is realised via a spontaneous emission coupling of the n qubits to a Bosonic field, and subsequently letting the qubits 'leak' into this environment. Since there is no correlation between atoms and field, the statistical model decouples into a Gaussian state $\Phi_{\mathbf{u}}$ associated to the field, and a classical statistical mixture of atoms, distributed according to $N_{\mathbf{u}}$. The corresponding operations of attenuation and amplification may then be carried out in the field in the optimal way.

In our case we need to consider mixed qubit states, which means that the collective state has non-zero components in all irreducible representations of $\text{SU}(2)$ (all values of the total spin). In fact the traces of the different blocks of given total spin form a probability distribution which (after centring and scaling) converges to the classical Gaussian component of the limit model in LAN. A typical block state of definite total spin can be mapped isometrically into the Fock space of a one mode CV system, and converges to the quantum Gaussian component of the limit model. This transfer can be implemented in principle by a creation-annihilation coupling with a Bosonic field in which the state 'leaks' after a short time. The classical part (total spin) can be measured by coupling subsequently with another Bosonic field, and performing an indirect measurement of L_z in the field. Since after the first step, all blocks are in the $|j, j\rangle$ state, a measurement of L_z is implicitly a measurement of the total spin.

The above convergence can be interpreted as follows: the quantum statistical models \mathcal{P}_n can be mapped into the Gaussian model \mathcal{N} and vice-versa, by means of physical operations (quantum channels) with vanishing norm-one error. From the statistical point of view, in many situations this convergence is strong enough to allow us to map a statistical problem concerning the model \mathcal{P}_n to a similar one concerning the simpler model \mathcal{N} .

In the case of purification or dilution of qubits, the mapping into a Gaussian problem is illustrated in the diagram below. We first give a detailed description of the steps involved, and then prove that our procedure is optimal (asymptotically minimax).

$$\begin{array}{ccc} \rho_{\mathbf{r}_0 + \frac{\mathbf{u}}{\sqrt{n}}}^{\otimes n} & \xrightarrow{Q_n^*} & \rho_{\lambda \mathbf{r}_0 + \frac{\mathbf{u}'}{\sqrt{m}}}^{\otimes m} \\ T_n \downarrow & & \uparrow S_m \\ N_{\mathbf{u}} \otimes \Phi_{\mathbf{u}}^{s_1} & \xrightarrow{K^* \otimes P^*} & N_{\mathbf{u}'} \otimes \Phi_{\mathbf{u}'}^{s_2} \end{array} \quad (23)$$

Step 1: Localisation. We are given n identical qubits in an arbitrary mixed state $\rho_{\mathbf{r}}$. We measure a small proportion $n^{1-\epsilon} \ll n$ of the qubits, to obtain a rough estimator $\rho_{\mathbf{r}_0}$ of the state. By standard concentration results, with asymptotically vanishing probability of error, the actual state is in a local neighbourhood of $\rho_{\mathbf{r}_0}$ of size $n^{-1/2+\epsilon}$, so that the remaining qubits can be parametrised as in the local model (21). In the

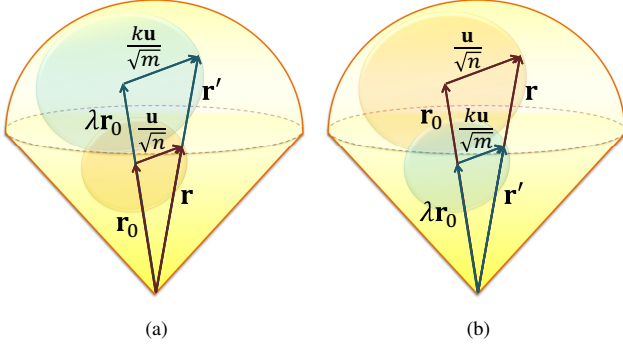


FIG. 4: (Color online) Schematic Bloch-sphere geometry for (a) purification and (b) dilution of qubits. A change in Bloch vector magnitude by factor λ is reflected by a change in the corresponding Gaussian state displacement. The two are then related by $\lambda = k\sqrt{n/m}$.

same time, the target single-system output state $\rho_{\lambda r}$ belongs to the local model

$$\mathcal{Q}_m := \left\{ \rho_{\lambda \mathbf{r}_0 + \frac{\mathbf{u}'}{\sqrt{m}}}^{\otimes m} : \|\mathbf{u}'\| \leq \lambda \Lambda^{1/2-\epsilon} m^\epsilon \right\}$$

with local parameter (see Figure 4)

$$\mathbf{u}' = \lambda \sqrt{\frac{m}{n}} \mathbf{u} = \lambda \Lambda^{1/2} \mathbf{u} := k \mathbf{u}.$$

Step 2: Transfer to the Gaussian state. We apply the map T_n to the qubits and obtain a classical random variable and a single-mode CV system whose states are approximately Gaussian [see (22)]

$$N_{\mathbf{u}} \otimes \Phi_{\mathbf{u}} = N(u_z, 1 - \|\mathbf{r}_0\|^2) \otimes W_{\alpha} \Phi^s W_{\alpha}^{\dagger}. \quad (24)$$

Step 3: Optimal Gaussian purification (amplification). Since \mathcal{Q}_m is a local model around $\lambda \mathbf{r}_0$, the corresponding parameter of the associated Gaussian model is

$$s_2 := \frac{1 - \lambda \|\mathbf{r}_0\|}{1 + \lambda \|\mathbf{r}_0\|}.$$

and the family of Gaussian states is

$$N(ku_z, 1 - \|k\mathbf{r}_0\|^2) \otimes W_{k\alpha} \Phi^{s_2} W_{k\alpha}^{\dagger}. \quad (25)$$

In this step we attenuate (amplify) the Gaussian state (24) in order to map it into, or close to (25), as described in Section II. This means that we apply the optimal channel K^* defined in section II A to the classical component $N_{\mathbf{u}}$, and the optimal quantum attenuation (amplification) channel P^* defined in Theorem II.1, to the quantum Gaussian component $\Phi_{\mathbf{u}}$.

Step 4: Mapping back to the qubits. We apply the channel S_m to the classical variable and the output of the attenuation (amplification) channel to obtain a state of m qubits in the neighbourhood of the state $\rho_{\lambda \mathbf{r}_0}$.

By composing the channels employed in steps 2–4 we obtain the overall channel

$$Q_n := S_n \circ (K^* \otimes P^*) \circ T_n,$$

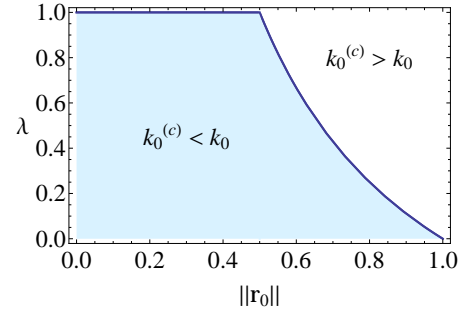


FIG. 5: (Color online) Parameter range defining the different regimes of qubit dilution. In the shaded region below the boundary curve $\lambda = \tilde{\lambda}(\|\mathbf{r}_0\|)$ [Eq. (27)], the threshold $k_0^{(c)}$ for a nonzero classical Gaussian risk is smaller than the corresponding threshold k_0^{amp} for a nonzero quantum Gaussian risk, and Cases 3 and 4 of Theorem III.1 apply for determining the optimal FoM for the qubit problem. Above the boundary curve, the situation is reversed, and Cases 2 and 4 of Theorem III.1 apply instead.

which will be shown to be optimal. Recall that for $k \leq k_0$ [see Eq. (12)], the quantum component $\Phi_{k\alpha}^{s_2}$ of the Gaussian target state can be prepared exactly. The same is true for the classical component when $k \leq k_0^{(c)}$, where

$$k_0^{(c)} = \sqrt{\frac{1 - \lambda^2 \|\mathbf{r}_0\|^2}{1 - \|\mathbf{r}_0\|^2}} \quad (26)$$

is obtained by substituting $V_1 = 1 - \|\mathbf{r}_0\|^2$, $V_2 = 1 - \lambda^2 \|\mathbf{r}_0\|^2$ for the variances in (4).

This means that the total risk has different expressions over the following three intervals: it is zero when $0 < k \leq \min(k_0, k_0^{(c)})$, it has one classical or quantum contribution for $\min(k_0, k_0^{(c)}) < k \leq \max(k_0, k_0^{(c)})$ and has both quantum and classical contributions for $k > \max(k_0, k_0^{(c)})$. For purification (corresponding to Gaussian attenuation), the ordering $0 < k_0^{\text{att}} < k^{(c)} < 1$ always holds, so the middle interval has a quantum contribution. However, for dilution (corresponding to Gaussian amplification), the ordering of k_0 and $k_0^{(c)}$ depends on the parameters $\|\mathbf{r}_0\|$ and λ . In particular, we see the appearance of a boundary which demarcates the two separate regimes of dilution, each defined by whether classical or quantum contributions to the risk take place first (see Fig. 5). Namely, $k_0^{(c)} < k_0^{\text{amp}}$ for

$$\lambda < \tilde{\lambda}(\|\mathbf{r}_0\|) \equiv \min \left\{ 1, \frac{1 - \|\mathbf{r}_0\|}{\|\mathbf{r}_0\|} \right\}, \quad (27)$$

and $k_0^{(c)} \geq k_0^{\text{amp}}$ otherwise. Notice that inequality (27) is always satisfied for $\|\mathbf{r}_0\| \leq 1/2$ for all values of λ .

The relation between the output qubit rate $\Lambda = m/n$ and the constants λ, k can be inferred from the geometry of the Bloch sphere (see Fig. 4)

$$\Lambda(\|\mathbf{r}_0\|, \lambda, k) = \frac{k^2}{\lambda^2}. \quad (28)$$

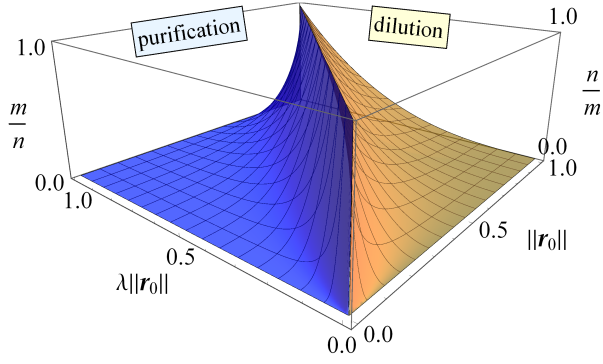


FIG. 6: (Color online) Optimal input (n) vs output (m) rates Λ_0 of qubit production for the processes of perfect purification and dilution, [Eq. (29)], plotted versus the Bloch vector lengths before ($\|\mathbf{r}_0\|$) and after ($\lambda\|\mathbf{r}_0\|$) the protocols. The left (right) side of the three-dimensional surface, corresponding to the region $\lambda > 1$ ($\lambda < 1$), represents the optimal rate m/n (n/m) for mixed qubit purification (dilution).

In particular, the maximum output rates for which the asymptotic risk is zero are obtained by setting: $k = k_0^{\text{att}}$ for purification, and

$$k = \begin{cases} k_0^{(c)}, & \lambda < \tilde{\lambda}(\|\mathbf{r}_0\|), \\ k_0^{\text{amp}}, & \text{otherwise,} \end{cases}$$

for dilution.

Explicitly,

$$\begin{aligned} \Lambda_0^{\text{pur}}(\|\mathbf{r}_0\|, \lambda) &= \frac{\lambda^{-1} - \|\mathbf{r}_0\|}{\lambda^2(1 - \|\mathbf{r}_0\|)}; \\ \Lambda_0^{\text{dil}}(\|\mathbf{r}_0\|, \lambda) &= \begin{cases} \frac{\lambda^{-2} - \|\mathbf{r}_0\|^2}{1 - \|\mathbf{r}_0\|^2}, & \lambda < \tilde{\lambda}(\|\mathbf{r}_0\|), \\ \frac{\|\mathbf{r}_0\| + 1/\lambda}{\lambda^2(\|\mathbf{r}_0\| + 1)}, & \text{otherwise.} \end{cases} \end{aligned} \quad (29)$$

The optimal rates (29) are plotted in Fig. 6.

We can now state main result of this section whose proof is given in Appendix A.

Theorem III.1. *The sequence of purification (dilution) maps*

$$Q_n^* := S_m \circ (K^* \otimes P^*) \circ T_n \quad (30)$$

is locally asymptotically minimax.

We distinguish four cases for the minimax risk.

Case 1: *Zero risk. If $k < \min(k_0, k_0^{(c)})$ then the minimax risk is zero. The optimal output rate Λ_0 is given in (29).*

Case 2: *Quantum contribution. If $k_0 \leq k \leq k_0^{(c)}$, then the purification (dilution) minimax risk at \mathbf{r}_0 is equal to the risk of the optimal Gaussian attenuation (amplification) scheme (14)*

$$R_{\text{minmax}}(\mathbf{r}_0, \lambda, \Lambda) = R_{\text{minmax}}(k, s_1, s_2). \quad (31)$$

Case 3: *Classical contribution. If $k_0^{(c)} \leq k \leq k_0$, then the dilution minimax risk at \mathbf{r}_0 is equal to the risk of the optimal*

classical Gaussian amplification scheme (5):

$$R_{\text{minmax}}(\mathbf{r}_0, \lambda, \Lambda) = R_{\text{minmax}}(V_1, V_2, k). \quad (32)$$

Case 4: *Classical and quantum contributions. If $k > \max(k_0, k_0^{(c)})$, then the purification (dilution) minimax risk is*

$$\begin{aligned} R_{\text{minmax}}(\mathbf{r}_0, \lambda, \Lambda) &= \int dx \sum_n \left| \frac{\exp\left(-\frac{x^2}{2k^2(1-\|\mathbf{r}_0\|^2)}\right)(1-\tilde{s})\tilde{s}^n}{\sqrt{2\pi k^2(1-\|\mathbf{r}_0\|^2)}} \right. \\ &\quad \left. - \frac{\exp\left(-\frac{x^2}{2(1-\lambda^2\|\mathbf{r}_0\|^2)}\right)(1-s_2)s_2^n}{\sqrt{2\pi(1-\lambda^2\|\mathbf{r}_0\|^2)}} \right| \end{aligned} \quad (33)$$

where \tilde{s} takes the values given in (15) in the case of attenuation (for qubit purification) and amplification (for qubit dilution) respectively.

The optimal minimax risk for purification and dilution of qubits is plotted in Fig. 7 as a function of k .

IV. CONCLUSIONS

We have solved the practically relevant problem of optimal attenuation and amplification of displaced Gaussian states, with respect to the maximum norm-one distance FoM. As expected, the optimal channels are implemented by the beam-splitter and parametric amplifier respectively, where the ancillary state is provided by the vacuum in both cases. This solution was then used in conjunction with LAN, to construct optimal purification and dilution channels for ensembles of i.i.d. qubits as formulated in Theorem III.1.

In the Gaussian case, we give an explicit expression of the FoM as a function of the variance parameters s_1 and s_2 of input and output states and the attenuation (amplification) factor k . In particular we identify the optimal value $k_0(s_1, s_2)$ for which the protocol achieves the target state exactly. Similarly, in the multiple qubits case, we derive the FoM as a function of the input and output purity and the asymptotic input/output rate Λ , and identify the optimal rate Λ_0 for which the protocol achieves the target collective state exactly. Both classical and quantum Gaussian contributions to the risk have to be taken into account to calculate the maximum rates, and to provide the optimal FoM for purification and dilution of multiple qubits, in the parameter range where the procedures cannot be accomplished perfectly.

An interesting future project is to extend the techniques used in this paper to tackle the general problem of asymptotically optimal channel inversion for arbitrary channels on finite dimensional systems. Such a study may provide efficient strategies to counteract the effect of various types of noise and decoherence processes, beyond the depolarising channel considered in the present work.

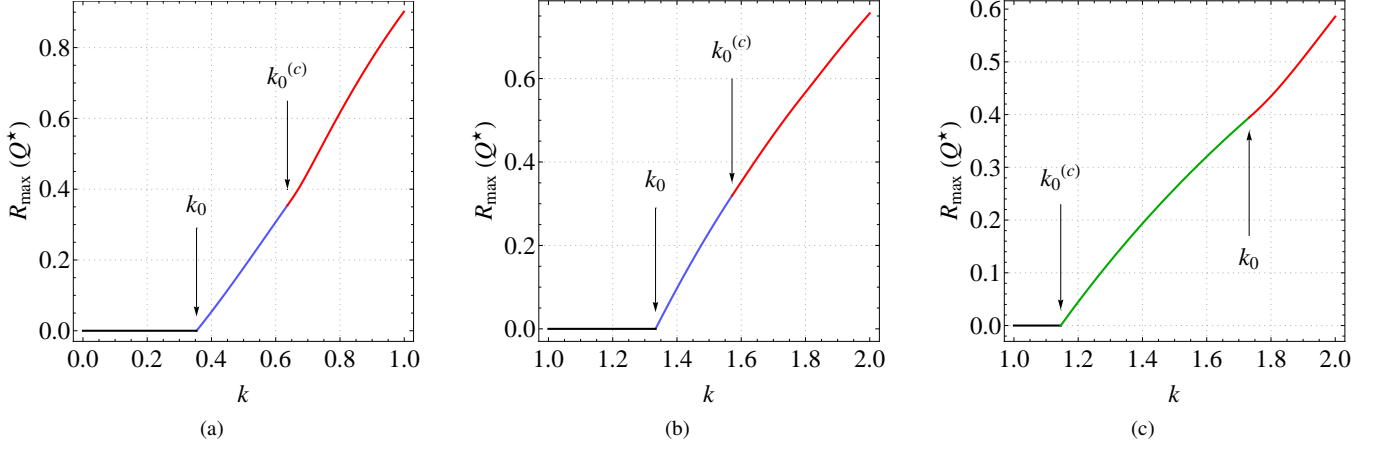


FIG. 7: (Color online) Plot of the minimax risk $R_{\max}(Q^*)$ [Eqs. (31–33)] for (a) optimal purification with $\|\mathbf{r}_0\| = 1/3$, $\lambda\|\mathbf{r}_0\| = 4/5$, (b) optimal dilution with $\|\mathbf{r}_0\| = 4/5$, $\lambda\|\mathbf{r}_0\| = 1/3$, and (c) optimal dilution with $\|\mathbf{r}_0\| = 1/2$, $\lambda\|\mathbf{r}_0\| = 1/8$, of n qubits, as a function of the local scale factor k . In panels (a) and (b), the risk is zero for $k < k_0$ (black line), it is given by the quantum Gaussian FoM for $k_0 \leq k < k_0^{(c)}$ (blue line, corresponding to Case 2 of Theorem III.1), and it is then given by the joint quantum and classical contributions for $k \geq k_0^{(c)}$ (red line, corresponding to Case 4 of Theorem III.1). In panel (c), which describes a dilution characterised by a choice of parameters within the shaded region of Fig. 5, we have instead that the risk is zero for $k < k_0^{(c)}$ (black line), it is given by the classical Gaussian FoM for $k_0^{(c)} \leq k < k_0$ (green line, corresponding to Case 3 of Theorem III.1), and it is then given by the joint quantum and classical contributions for $k \geq k_0$ (red line, corresponding to Case 4 of Theorem III.1).

Acknowledgments

Mădălin Guță was supported by the EPSRC Fellowship EP/E052290/1.

Appendix A: Proofs

Proof of Theorem II.1

Proof. As the proof follows the lines of similar results in [14, 21] we will briefly sketch the main ideas. A covariance argument [27, 28] shows that one may restrict the attention to channels which are displacement-covariant, in the sense that $P(W_\xi \Phi W_\xi^\dagger) = W_\xi P(\Phi) W_\xi^\dagger$ for any input state ρ . For such channels the risk is independent of α and

$$R_{\max}(k, s_1, s_2, P) = \|P(\Phi^{s_1}) - \Phi^{s_2}\|_1$$

In the case of attenuation ($k < 1$) such channels are described by the linear transformation

$$c_{\text{att}} = ka + \sqrt{1 - k^2}b$$

where a is the input mode, c_{att} is the output and b is an ancillary mode prepared in a state τ . Since the channel is completely characterised by the state τ , we will denote it by P_τ . Similarly, for amplification ($k > 1$) the output of the channel P_τ is the mode

$$c_{\text{amp}} = ka + \sqrt{k^2 - 1}b^\dagger,$$

with b prepared in the state τ . By a second covariance argument with respect to phase rotations, and taking into account that Φ is invariant under phase rotations, we obtain that τ can be taken to be phase-invariant, i.e. it is a mixture of Fock states $\tau = \sum_i \tau_i |i\rangle\langle i|$. In this case the output state will be diagonal in the Fock basis and we write $P_\tau(\Phi^{s_1}) = \sum_i p_i^\tau |i\rangle\langle i|$, and in particular p^ω corresponds to the output state when the ancilla is the vacuum. Similarly, we denote the coefficients of the Gaussian state Φ^{s_1} and Φ^{s_2} by $p_i = (1 - s_1)s_1^i$ and $q_i = (1 - s_2)s_2^i$. The proof reduces now to showing that, for any τ ,

$$\|p^\tau - q\|_1 \geq \|p^\omega - q\|_1. \quad (\text{A1})$$

The key to proving this statement is the concept of stochastic ordering, whose definition we recall:

Definition A.1 (Stochastic Ordering). *Let $p = \{p_l : l \in \mathbb{N}\}$ and $q = \{q_l : l \in \mathbb{N}\}$ be two probability distributions over \mathbb{N} . We say that p is stochastically smaller than q ($p \preceq q$) if*

$$\sum_{l=0}^m p_l \geq \sum_{l=0}^m q_l, \quad \forall m \geq 0 \quad (\text{A2})$$

The following lemma holds for both the purification and the amplification scenarios:

Lemma A.2. *For any state τ the following stochastic ordering holds*

$$p^\omega \preceq p^\tau. \quad (\text{A3})$$

Proof. We treat the attenuation and amplification separately but the idea is the same in both cases: we reduce the statement about stochastic ordering to a simpler one where the input mode is in the vacuum.

Attenuation. We write the input mode as $a = \cosh(t)a_1 + \sinh(t)a_2^\dagger$ with $a_{1,2}$ two fictitious modes in the vacuum state, and $\tanh^2(t) := s_1$, which ensures that the state of a is Φ^{s_1} . Let \tilde{t} be such that $\sinh(\tilde{t}) = k \sinh(t)$ and denote

$$T = \sqrt{1 - \frac{(1-k^2)}{\cosh^2(\tilde{t})}}, \quad R = \frac{\sqrt{1-k^2}}{\cosh(\tilde{t})}.$$

Then $c_{pur} = ka + \sqrt{1-k^2}b$ can be written as

$$\begin{aligned} c_{pur} &= \cosh(\tilde{t})(Ta_1 + Rb) + \sinh(\tilde{t})a_2^\dagger \\ &= \cosh(\tilde{t})\tilde{b} + \sinh(\tilde{t})\tilde{a}^\dagger \end{aligned}$$

where $\tilde{b} := Ta_1 + Rb$ and a_2 was relabelled \tilde{a} . The state of the mode \tilde{b} is given by

$$\begin{aligned} \tilde{\tau} &= \sum_{k=0}^{\infty} \tau_k \sum_{p=0}^k \binom{k}{p} T^{2(p-k)} R^{2k} |p\rangle\langle p| \\ &= \sum_{p=0}^{\infty} \tilde{\tau}_p |p\rangle\langle p| \end{aligned}$$

so \tilde{b} is in the vacuum state if and only if b is in the vacuum. Thus it suffices to prove the stochastic ordering statement for the mode c_{att} written as a combination of \tilde{b} and \tilde{a} for an arbitrary diagonal state $\tilde{\tau}$ of \tilde{b} and \tilde{a} in the vacuum. Furthermore, since stochastic ordering is preserved under convex combinations, it suffices to prove the statement for any *pure* diagonal state $\tilde{\tau} = |k\rangle\langle k|$, $k \neq 0$. In this case the state of c_{att} is given by

$$\begin{aligned} \rho_{att}^{out} &= e^{-2g(k+1)} \sum_{l=0}^{\infty} \Gamma^{2l} \binom{l+k}{k} |l+k\rangle\langle l+k| \\ &:= \sum_{l=0}^m d_l^{(k)} |l+k\rangle\langle l+k| \end{aligned}$$

where $\Gamma = \tanh(\tilde{t})$ and $e^g = \cosh(\tilde{t})$. The stochastic ordering now reduces to showing that $\sum_{l=0}^m d_l^{(0)} \geq \sum_{l=0}^m d_l^{(k)}$ for all m . With the notation $\gamma = \Gamma^2$, we get

$$\begin{aligned} \sum_{l=0}^{p+k} d_l^{(k)} &= (1-\gamma)^{k+1} \sum_{l=0}^p \gamma^l \binom{l+k}{k} \\ &\leq 1 - \gamma^{p+1} \sum_{r=0}^k (1-\gamma)^r \gamma^{k-r} \binom{k}{r} \\ &= 1 - \gamma^{p+1} = \sum_{l=0}^p d_l^{(0)}. \end{aligned}$$

Amplification. As before we write $a = \cosh(t)a_1 + \sinh(t)a_2^\dagger$ and define \tilde{t} by $\cosh(\tilde{t}) = k \cosh(t)$ and the beam-splitter coefficients

$$T = \sqrt{1 - \frac{(1-k^2)}{\sinh^2(\tilde{t})}}, \quad R = \frac{\sqrt{1-k^2}}{\sinh(\tilde{t})}.$$

The output mode is now

$$\begin{aligned} c_{amp} &= \sinh(\tilde{t})(Rb^\dagger + Ta_2^\dagger) + \cosh(\tilde{t})a_1 \\ &= \sinh(\tilde{t})\tilde{b}^\dagger + \cosh(\tilde{t})\tilde{a} \end{aligned}$$

where we have relabelled a_1 by \tilde{a} and introduced the mode $\tilde{b} = Rb^\dagger + Ta_2^\dagger$. As before, the state of \tilde{b} is the vacuum if and only if b is in the vacuum state, so it suffices to verify the statement for the state $\tilde{\tau} = |k\rangle\langle k|$ in which case the output state is

$$\rho_{amp}^{out} = e^{-2g(k+1)} \sum_{l=0}^{\infty} \Gamma^{2l} \binom{l+k}{k} |l\rangle\langle l| = \sum_{l=0}^m d_l^{(k)} |l\rangle\langle l|$$

The relation $p^\omega \preceq p^\tau$ now follows from

$$\begin{aligned} \sum_{l=0}^p d_l^{(k)} &= (1-\gamma)^{k+1} \sum_{l=0}^p \gamma^l \binom{l+k}{k} \\ &\leq 1 - \gamma^{p+1} = \sum_{l=0}^p d_l^{(0)}. \end{aligned}$$

This ends the proof of Lemma A.2 for both cases. \square

The following lemma completes the proof of Theorem II.1 by transforming the stochastic ordering into the desired norm inequality (A1). Its proof [14, 21] uses the fact that $q \preceq p^\omega$ which is equivalent to the fact that $P^*(\Phi^{s_1})$ is more noisy than Φ^{s_2} . The latter is satisfied for $k \geq k_0$ as assumed in the theorem.

Lemma A.3. *Let p' be a discrete probability distribution such that $p^\omega \preceq p'$. Then*

$$\|p' - q\|_1 \geq \|p^\omega - q\|_1. \quad (\text{A4})$$

\square

Proof of Lemma II.2

We use the notations introduced in the proof of Theorem II.1. By expressing the quadrature variance of the input mode a in terms of t and s_1 we obtain $\sinh^2 t = \frac{1}{e^{s_1}-1}$. According to Theorem II.1 the output state of the optimal channel P^* is the Gaussian state

$$P^*(\Phi^{s_1}) = \Phi^{\tilde{s}} = e^{-2g} \sum_{l=0}^{\infty} (1 - e^{-2g})^l |l\rangle\langle l|$$

with g taking different values in the attenuation and amplification cases. For the geometric distributions p^ω and q we have

$$\|\Phi^{\tilde{s}} - \Phi^{s_2}\|_1 = \|p^\omega - q\|_1 = 2(\tilde{s}^{m_0+1} - s_2^{m_0+1})$$

where m_0 is the largest integer such that $p_{m_0}^\omega \leq q_{m_0}$, more precisely

$$m_0 = \lfloor \ln[(1-\tilde{s})/(1-s_2)] / \ln(s_2/\tilde{s}) \rfloor$$

It remains to compute the concrete expressions of \tilde{s} and implicitly of m_0 for the attenuation and amplification cases. For attenuation, making use of $\sinh \tilde{t} = k \sinh t$, we find

$$\tilde{s}_{pur} = \frac{s_1 k^2}{1 - s_1 + s_1 k^2}.$$

For amplification, we use $\cosh \tilde{t} = k \cosh t$ and find

$$\tilde{s}_{amp} = 1 - \frac{1 - s_1}{k^2}.$$

Proof of Theorem III.1

Proof. We want to show that $Q^* := S_n \circ P^* \circ T_n$ is the optimal purification or dilution procedure for n i.i.d. qubits. The idea is that, by using LAN, we can show the qubit and Gaussian statistical problems to be equivalent, the Gaussian one (respectively for attenuation and amplification) being solved in Section II B, which then allows us to recast the qubit problem in the Gaussian setup with a vanishing difference in the risks. We will consider the four separate cases: zero risk, solely quantum contribution, solely classical contribution, and both classical and quantum contributions. We will then use the Gaussian solution to show that $R_{\max}(\mathbf{r}_0, Q^*, \lambda)$ is less than or equal to the corresponding optimal Gaussian risk, then show that a strict inequality violates the optimality of this optimal solution. We begin by restricting \mathbf{r} to the local neighbourhood $\|\mathbf{r} - \mathbf{r}_0\| \leq n^{-\frac{1}{2} + \epsilon}$. This probability that the state fails to be in this region is $o(1)$ and has no influence on the asymptotic risk (see Lemma 2.1. in [10]). We are now able to apply LAN, which maps input states $\rho_{\mathbf{r}}^{\otimes n}$ close to some Gaussian state, say $\tilde{\Phi}_{\mathbf{u}}$, via the channel T_n . We now consider the individual cases, which are each slight variations on the same proof:

Case1: $k < \min(k_0, k_0^{(c)})$. In this case both classical and quantum Gaussian channels have zero risk, so the asymptotic qubit risk is zero.

Case 2: $k_0 \leq k \leq k_0^{(c)}$. In this instance, the risk receives only a quantum contribution. Using contractivity of the CP maps S_m and P^* , the LAN convergence, and the fact that in this regime $K^* N_{\mathbf{u}} = N_{\mathbf{u}'}$ we obtain

$$\begin{aligned} R(Q_n^*, \mathbf{r}, \lambda) &= \|\rho_{\mathbf{u}'}^m - Q_n^*(\rho_{\mathbf{u}}^n)\|_1 \\ &\leq \|\rho_{\mathbf{u}'}^m - S_m(\Phi_{\mathbf{u}'}^{s_2} \otimes N_{\mathbf{u}'})\|_1 \\ &\quad + \|S_m(\Phi_{\mathbf{u}'}^{s_2} \otimes N_{\mathbf{u}'}) - S_m(P^* \otimes K^*(T_n(\rho_{\mathbf{u}}^n)))\|_1 \\ &\leq \|\Phi_{\mathbf{u}'}^{s_2} \otimes N_{\mathbf{u}'} - P^* \otimes K^*(T_n(\rho_{\mathbf{u}}^n))\|_1 + o(1) \\ &= \|\Phi_{\mathbf{u}'}^{s_2} \otimes N_{\mathbf{u}'} - P^* \otimes K^*(\Phi_{\mathbf{u}}^{s_1} \otimes N_{\mathbf{u}})\|_1 + o(1) \\ &= \|\Phi_{\mathbf{u}'}^{s_2} - P^*(\Phi_{\mathbf{u}}^{s_1})\|_1 + o(1) \\ &= R_{\min\max}(s_1, s_2, k) + o(1) \end{aligned} \quad (\text{A5})$$

where $R_{\min\max}(s_1, s_2, k)$ is the minimax risk for the quantum Gaussian problem, obtained in Theorem II.1. By taking supremum over $\|\mathbf{u}\| < n^\epsilon$ we get

$$R_{\max}(Q_n^*, \mathbf{r}_0, \lambda) \leq R_{\min\max}(s_1, s_2, k).$$

which implies that

$$R_{\min\max}(\mathbf{r}_0, \lambda) \leq R_{\min\max}(s_1, s_2, k).$$

Next, we show by contradiction that this inequality cannot be strict. Suppose that there exists a sequence of purification or dilution procedures \tilde{Q}_n , which act on qubits and satisfies $R_{\max}(\tilde{Q}_n \mathbf{r}_0, \lambda) \leq R_{\min\max}(s_1, s_2, k) - \eta$ for some $\eta > 0$ and $n > n_0$. We will use LAN to show that there exists a Gaussian dilution (amplification) channel whose risk is strictly smaller than the minimax risk, which is a contradiction.

The general setup can be seen in (A6)

$$\begin{array}{ccc} \rho_{\mathbf{u}}^{\otimes n} & \xrightarrow{\tilde{Q}_n} & \rho_{\lambda \mathbf{r}}^{\otimes m} \\ \uparrow S_n & & T_m \downarrow \\ \Phi_{\mathbf{u}}^{s_1} & \xrightarrow{\tilde{P}} & \Phi_{k\alpha}^{s_2} \end{array} \quad (\text{A6})$$

Here LAN is restricted to a *two dimensional* family of rotated qubit states, for which the limit model is quantum Gaussian, with no classical component. Assuming $\Phi_{\mathbf{u}}^{s_1}$ is in the domain of applicability of LAN (which can be effected by an adaptive measurement [14]), we get the inequalities

$$\begin{aligned} \|T_m \circ \tilde{Q}_n \circ S_n(\Phi_{\mathbf{u}}^{s_1}) - \Phi_{\mathbf{u}'}^{s_2}\| &\leq \|\tilde{Q}_n(\rho_{\mathbf{u}}^n) - \rho_{\mathbf{u}'}^m\|_1 + \|T_m(\rho_{\mathbf{u}'}^m) - \Phi_{\mathbf{u}'}^{s_2}\|_1 \\ &\leq R_{\min\max}(s_1, s_2, k) - \eta + o(1). \end{aligned} \quad (\text{A7})$$

By taking the limit $n \rightarrow \infty$ we get the desired contradiction.

Case 3: $k_0^{(c)} \leq k \leq k_0$. This case applies only to dilution and the risk receives only a classical contribution. The proof follows the same steps as the previous case, with the quantum Gaussian replaced by the classical one. The inequality (A5) becomes

$$\begin{aligned} R(Q_n^*, \mathbf{r}, \lambda) &= \|\rho_{\mathbf{u}'}^m - Q_n^*(\rho_{\mathbf{u}}^n)\|_1 \\ &\leq \|N(0, 1 - \lambda^2 \|\mathbf{r}_0\|^2) - K^*(N(0, 1 - \|\mathbf{r}_0\|^2))\|_1 + o(1) \\ &= R_{\min\max}(V_1, V_2, k) + o(1). \end{aligned} \quad (\text{A8})$$

where $R_{\min\max}(V_1, V_2, k)$ is the optimal risk of Eq. (5) and we have identified $V_1 = 1 - \|\mathbf{r}_0\|^2$, $V_2 = 1 - \lambda^2 \|\mathbf{r}_0\|^2$. This implies

$$R_{\min\max}(\mathbf{r}_0, \lambda) \leq R_{\min\max}(V_1, V_2, k).$$

The equality is obtained by showing that strict inequality would lead to a classical amplification procedure whose risk is smaller than the minimax risk.

Case 4: $k > \max(k_0^{(c)}, k_0)$. This case applies to both dilution and amplification, and both the quantum and classical channels contribute to the risk.

$$\begin{aligned} R_{\max}(Q_n^*, \mathbf{r}, \lambda) &= \|\rho_{\mathbf{u}'}^m - Q_n^*(\rho_{\mathbf{u}}^n)\|_1 \\ &\leq \|\Phi_{\mathbf{u}'}^{s_2} \otimes N_{\mathbf{u}'} - K^* \otimes P^*(\Phi_{\mathbf{u}}^{s_1} \otimes N_{\mathbf{u}})\|_1 + o(1) \\ &\leq R_{\min\max}(V_1, V_2, s_1, s_2, k) + o(1). \end{aligned} \quad (\text{A9})$$

Here $R_{\min\max}(V_1, V_2, s_1, s_2, k)$ is the minimax norm-one risk for the problem of transforming the Gaussian state $\Phi_{\mathbf{u}}^{s_1} \otimes N_{\mathbf{u}}$ into $\Phi_{\mathbf{u}'}^{s_2} \otimes N_{\mathbf{u}'}$. Since the quantum and classical components are independent and have different local parameters, the optimal channel is the product $K^* \otimes P^*$. The explicit expression of the minimax risk is

$$\begin{aligned}
 & R_{\min\max}(V_1, V_2, s_1, s_2, k) \\
 &= \int dx \sum_n \left| \frac{\exp\left(-\frac{x^2}{2k^2(1-\|\mathbf{r}_0\|^2)}\right)}{\sqrt{2\pi k^2(1-\|\mathbf{r}_0\|^2)}} (1-\tilde{s})\tilde{s}^n \right. \\
 & \quad \left. - \frac{\exp\left(-\frac{x^2}{2(1-\lambda^2\|\mathbf{r}_0\|^2)}\right)}{\sqrt{2\pi(1-\lambda^2\|\mathbf{r}_0\|^2)}} (1-s_2)s_2^n \right| \quad (\text{A10})
 \end{aligned}$$

Finally, the equality in (A9) can be proven by contradiction as in case 2. \square

-
- [1] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, Phys. Rev. Lett. **76**, 722-725 (1996).
 - [2] A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
 - [3] J.I. Cirac, A.K. Ekert, and C. Macchiavello, Phys. Rev. Lett. **82**, 4344 (1999).
 - [4] M. Keyl and R. F. Werner, Annales Henri Poincaré **2**, 1 (2001).
 - [5] G.M. D'Ariano, C. Macchiavello, and P. Perinotti, Phys. Rev. Lett. **95**, 060503 (2005).
 - [6] M. Ricci, F. De Martini, N.J. Cerf, R. Filip, J. Fiurasek and C. Macchiavello Phys. Rev. Lett. **93**, 170501 (2004).
 - [7] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
 - [8] L. Le Cam, *Asymptotic Methods in Statistical Decision Theory* (Springer Verlag, New York, 1986).
 - [9] M. Guță and J. Kahn, Phys. Rev. A **73**, 052108 (2006).
 - [10] M. Guță, B. Janssens, and J. Kahn, Commun. Math. Phys. **277**, 127 (2008).
 - [11] J. Kahn and M. Guță, Commun. Math. Phys. **289**, 597 (2009).
 - [12] M. Guță and A. Jenccová, Commun. Math. Phys. **276**, 341 (2007).
 - [13] M. Guță, B. Janssens and J. Kahn Commun. Math. Phys. **276**, 341 (2007).
 - [14] M. Guță, P. Bowles, and G. Adesso, Phys. Rev. A **82**, 042310 (2010).
 - [15] M. Guță and W. Kotłowski, New J. Phys. **12**, 12303 (2010).
 - [16] U.L. Andersen, R. Filip, J. Fiurasek, V. Josse and G. Leuchs Phys. Rev. A **72**, 060301 (2005).
 - [17] H.A. Haus and J.A. Mullen, Phys. Rev. **128**, 2407 (1962).
 - [18] C.M. Caves Phys. Rev. D **26**, 1817 (1982).
 - [19] A.A. Clerk, M.H. Devoret, S.M. Girvin, F. Marquardt, and R.J. Schoelkopf, Rev. Mod. Phys. **82**, 1155 (2008).
 - [20] Z. Y. Ou, S. F. Pereira, and H. J. Kimble, Phys. Rev. Lett. **70**, 3239 (1993).
 - [21] M. Guță and K. Matsumoto, Phys. Rev. A **74**, 032305 (2006).
 - [22] E.K. Torgersen, *Comparison of statistical experiments* (Cambridge University Press, 1991).
 - [23] J. Bae and A. Acin, Phys. Rev. Lett. **97**, 030402 (2006).
 - [24] A. W. Van Der Waart, *Asymptotic Statistics* (Cambridge University Press, Cambridge, UK, 1998)
 - [25] M. Guță and J. Kahn, in preparation.
 - [26] M. Guță, e-print arXiv:1007.0434 (2010).
 - [27] N.J. Cerf, O. Kruger, P. Navez, R.F. Werner, and M. M. Wolf, Phys. Rev. Lett. **95**, 070501 (2005).
 - [28] M. Owari, M. B. Plenio, E. S. Polzik, and A. Serafini, New J. Phys. **10**, 113014 (2008).